课本

1. 网络安全基础

1. 专业术语定义

2. 威胁模型

2.1. 微软STRIDE模型

2.1.1. 注意事项

2.2. 通用弱点评价体系CVSS

2.2.1. 相关标准与体系

2.3. DREAD模型

2.4. OCTAVE

2.5. 安全策略和安全机制

2.5.1. 信任和安全假设

2.5.2. 安全策略（Security Policy）

2.5.3. 安全机制（Security Mechanism）

2.6. 计算机网络安全模型

2.6.1. 静态模型——安全威胁的分层模型

2.6.2. 动态模型——P2DR模型

2.6.3. P2DR2动态安全模型

2.7. 等级安全保护

2.7.1. 等级安全保护的发展历史

2.7.2. 等级安全保护的必要性和意义

2.7.3. 等级安全保护的现状

2.8. 计算机安全法规

第二章 系统安全、风险评估理论与应用

1. 操作系统的简史

2. 数字标识理论

2.1. 定义

2.2. 意义

2.3. 常用的数字标识技术

2.3.1. 1. 系统实体标识

2.3.2. 2. 网络实体标识

3. 访问控制理论

3.1. 定义及组成

3.2. 访问控制的目的与内容

3.3. 访问控制策略

3.4. 访问控制机制

3.5. 从授权的角度看Windows7访问控制模型

4. 通用安全漏洞评估系统（CVSS）

4.1. CVSS的评估系统

4.2. 基本评估原则

4.3. 评估公式和评估过程

4.4. CVSS 3.0和CVSS 2.0

4.5. CVSS的局限性和不足

4.6. CVSS的应用

第三章 网络安全应用基础

1. 常见的代理服务

1.1. 基本概念

1.2. HTTP代理

1.2.1. HTTP的简单介绍

1.2.2. HTTP代理原理

1.2.3. HTTP代理的应用

1.2.4. HTTP代理的工作模式

1.2.5. HSTS - HTTP Strict Transport Security

1.3. 虚拟专用网（VPN）

1.3.1. 虚拟专用网的简介

1.3.2. VPN的应用与类型

1.3.3. VPN的设计原则

1.4. SOCKS代理

1.5. 小结

2. 高级代理服务

2.1. 匿名基本概念

2.2. 匿名通信

2.3. 匿名通信的实现

3. 代理服务的检测

3.1. 检测的需求与手段

3.2. 代理服务检测示例

第四章 网络监听

1. 网络监听原理

1.1. 被动监听

1.1.1. 共享式网络环境

1.2. 主动监听

1.2.1. 交换式网络环境

2. 网络监听工具

2.1. Wireshark简介

2.2. Wireshark功能和使用

2.3. dsniff简介

3. 网络监听的监测

3.1. 检测共享式网络环境中的监听者

3.2. 检测交换式网络环境中的监听者

3.2.1. 检测终端ARP缓存投毒者

3.2.2. 检测交换机DoS攻击

3.2.3. 检测交换机投毒者

4. 网络监听的防范

4.1. 终端用户的防范措施

4.2. 网络管理员的防范措施

第五章 网络扫描

1. 5.1 网络扫描与信息收集

1.1. 5.1.1 踩点

1.2. 5.1.2 扫描

1.3. 5.1.3 枚举

2. 5.2 网络扫描原理

2.1. 5.2.1 网络扫描的基本思想

2.2. 5.2.2网络扫描的基本原理

2.2.1. 5.2.2.1报文发送与接收

2.2.2. 5.2.2.2 扫描知识库的构建和规则匹配

2.2.3. 5.2.2.3 扫描报告的生成

2.3. 5.2.3 栈指纹OS识别技术

2.3.1. 5.2.3.1实现原理

2.3.2. 5.2.3.2 通过识别操作系统

2.3.3. 5.2.3.3栈指纹OS识别技术的其他技术

3. 5.3 网络扫描工具

3.1. 5.3.1 Nmap的简介

3.2. 5.3.2 Nmap使用方法

第六章 网络与系统渗透

1. 6.1 序曲

1.1. 6.1.1 引言

1.2. 6.1.2 基本概念

1.3. 6.1.3 网络安全

2. 6.2 网络与系统渗透的基本原理

2.1. 6.2.1 渗透测试

2.2. 6.2.2 入侵与预防

2.3. 6.2.3 案例一：从信息收集到入侵提权

2.4. 6.2.4 案例二：2012年新浪微博用户密码泄露漏洞（旁站注入）

2.5. 6.2.5 案例三：Google Hacking

2.6. 6.2.6 网络入侵的入口选择

第七章 WEB应用漏洞攻防

1. 7.1 输入有关的安全问题

2. 7.2 后台有关的安全问题

2.1. 7.2.1．注入缺陷

第八章

1. 8.1 概述

1.1. 8.1.1 防火墙的定义

1.2. 8.1.2 防火墙的发展简史

1.3. 8.1.3 防火墙现状与发展

2. 8.2 防火墙技术原理

2.1. 8.2.1 防火墙关键技术

2.1.1. 8.2.1.1包过滤技术

2.1.2. 8.2.1.2 状态检测技术

2.1.3. 8.2.1.3 代理服务技术

3. 8.3 防火墙的实现技术

3.1. 8.3.1 软件技术

3.1.1. 8.3.1.1 Netfilter/iptables框架简介

3.1.2. 8.3.1.2 Netfilter/iptable基本概念

3.1.3. 8.3.1.3 Netfilter/iptable防火墙工作原理

3.2. 8.3.2 硬件技术

4. 8.4 防火墙的配置和应用

4.1. 8.4.1 路由模式

4.2. 8.4.2 透明模式

4.3. 8.4.3 混合模式

4.4. 8.4.4 防火墙部署的其他细节

4.5. 8.4.5 单机防火墙的配置

4.5.1. 8.4.5.1 ufw

4.5.2. 8.4.5.2 iptables

5. 8.5 基于防火墙实现NAT

5.1. 8.5.1基本概念

5.2. 8.5.2 NAT工作原理

5.3. 8.5.3 使用实例

5.4. 8.5.4 iptables实现NAT综合实验

6. 8.6 防火墙规则调试和审查

6.1. 8.6.1 防火墙规则调试

6.2. 8.6.2 防火墙规则安全审查

第九章 入侵检测

1. 9.1 入侵检测概述

1.1. 9.1.1 发展简史

1.2. 9.1.2 入侵检测的意义和作用

2. 9.2 入侵检测理论

2.1. 9.2.1 入侵检测基本概念

2.2. 9.2.2 入侵检测技术

2.3. 9.2.3 入侵检测评价指标

3. 9.3 入侵检测关键技术

3.1. 9.3.1 基本技术

3.2. 9.3.2 入侵检测体系架构

4. 9.4 入侵检测标准化

4.1. 9.4.1通用入侵检测框架（CIDF）

4.2. 9.4.2 OPSEC（Open Platform for Security）

5. 9.5 入侵检测系统配置

5.1. 9.5.1入侵检测系统

5.2. 9.5.2 Snort

5.2.1. 9.5.2.1 Sonrt概述

5.2.2. 9.5.2.2 Snort规则

5.2.3. 9.5.2.3 Snort架构

5.3. 9.5.3 Suricata

5.4. 9.5.4 Bro

第十章 应用程序安全加固

1. 10.1 信息安全技术体系与威胁模型

1.1. 10.1.1 信息安全技术三维技术体系

1.2. 10.1.2 基于信息安全三维技术体系的安全加固

1.2.1. 10.1.2.1 从“功能”视角出发看安全加固

1.2.2. 10.1.2.2 从“目标”视角出发看安全加固

1.2.3. 10.1.2.3 从“时间”视角出发看安全加固

1.2.4. 10.1.2.4 安全加固的方法论小结

2. 10.2 操作系统安全加固

2.1. 10.2.1 围绕机密性目标

2.2. 10.2.2 围绕完整性目标

2.3. 10.2.3 围绕可用性目标

2.4. 10.2.4 围绕认证目标

2.5. 10.2.5 围绕授权目标

2.6. 10.2.6 围绕审计目标

2.7. 10.2.7 小结

3. 10.3 应用程序安全加固

3.1. 10.3.1 WEB服务器安全加固

3.2. 10.3.2 SSH服务器安全加固

3.3. 10.3.3 DNS服务器安全加固

4. 10.4 安全加固基准检查清单

第十一章 蜜罐和蜜网

1. 11.1 蜜罐发展史

1.1. 11.1.1 引言

1.2. 11.1.2 蜜罐概念和分类

1.3. 11.1.3 蜜罐实例

1.4. 11.1.4 蜜罐小结

2. 11.2 蜜罐关键技术

3. 11.3 蜜网技术

4. 11.4 蜜罐与蜜网技术的应用

第十二章 计算机取证

1. 12.1 计算机取证发展史

2. 12.2 计算机取证理论

2.1. 12.2.1 相关概念比较

2.2. 12.2.2 司法鉴定

2.2.1. 12.2.2.1 证据

2.2.2. 12.2.2.2 计算机证据的获取

2.2.3. 12.2.2.3 计算机证据的特点

2.3. 12.2.3 计算机证据理论

2.4. 12.2.4 计算机取证发展趋势

3. 12.3 计算机取证关键技术

3.1. 12.3.1 数据获取技术

3.2. 12.3.2 数据分析技术

3.3. 12.3.3 计算机犯罪分析

3.4. 12.3.4 数据解密技术

3.5. 12.3.5 证据保管

3.6. 12.3.6 证据（数据）校验

3.7. 12.3.7 反取证技术

4. 12.4 计算机取证案例学习

第十三章 社会化网络安全

1. 13.1 社会化网络基本概念

2. 13.2 社交网络安全

2.1. 13.2.1 社会工程学与网络钓鱼

2.2. 13.2.2 谣言

2.3. 13.2.3 恶意营销

3. 13.3 电信诈骗与防范

4. 13.4 电子商务网络安全

4.1. 13.4.1 消费端

4.2. 13.4.2 企业端

4.3. 13.4.3 平台端

5. 13.5 网络勒索

6. 13.6 大数据应用与隐私保护